HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/81C

24 August 2018

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Operational Incidents Watch

The Hong Kong Monetary Authority (HKMA) published today the ninth issue of the Operational Incidents Watch (see enclosure).

The Operational Incidents Watch is a periodic newsletter which highlights the major lessons learnt from selected significant operational incidents that have happened in the banking sector. It aims to help authorized institutions (AIs) and members of the public to stay alert and to take appropriate measures to prevent similar incidents from happening to them. The HKMA expects the senior management of AIs to take steps to ensure that their business lines or operational risk management functions will take into account the incidents described in the Operational Incidents Watch in reviewing and enhancing their risk management controls.

If there are any questions about the Operational Incidents Watch, please contact Ms Rachel Wan at 2878-8297 or Ms Christie Yee at 2878-1620.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Encl

55th Floor, Two International Finance Centre,
8 Finance Street, Central, Hong Kong
Website: www.hkma.gov.hk

香港中環金融街8號國際金融中心2期55樓
網址：www.hkma.gov.hk

Issue No. 9
24 August 2018

Operational Incidents Watch is a periodic newsletter published by the Banking Supervision Department of the Hong Kong Monetary Authority (HKMA). It summarises the major lessons learnt from selected operational incidents[1] that have happened in the banking industry and resulted in impact on customers or material financial losses to the banks concerned. It aims at facilitating banks and members of the public to stay alert and to take appropriate measures to prevent similar incidents from happening to them.

In this newsletter, the modus operandi or the factors and key control loopholes leading to two operational incidents are outlined. These incidents involved: (a) phishing emails and fraudulent bank websites stealing customers' e-banking account information; and (b) account takeover by a fraudster using a lost HKID card.

Phishing emails and fraudulent bank websites stealing customers' e-banking account information

The HKMA has observed an increasing number of cases involving fraudsters using phishing emails and fraudulent websites to deceive banking customers to disclose e-banking account information. In some cases, the customers suffered significant financial losses.

Modus operandi / factors leading to the incident

The fraudsters set up a fraudulent website purporting to be the official website of a bank and sent phishing emails with a subject line giving a sense of urgency (e.g. the recipients have to activate new features in order to continue using certain

[1] Because of sensitivity, the incidents mentioned in this newsletter may be prepared on the basis of synthesis of multiple incidents and certain details of the incidents may deliberately be omitted or altered.

banking services) to the potential victims. The recipients of the e-mail were urged to click on a hyperlink in the phishing email to update their e-banking account information. One victim, being an e-banking customer of the bank, followed the email's instructions and clicked the hyperlink. He was then directed to a fake website and provided his e-banking username, password, mobile phone number and other e-banking account information. The victim was unaware of the scam because the fake website appeared to be the same as the bank's official website. Once the fraudsters obtained the e-banking account information, they conducted unauthorized financial transactions out of the victim's account.

In some other cases, a phishing email pretending to be a notification of an outgoing fund transfer was sent with malicious attachments that can implant a malware into the victim's computer when he opened the attachments. The malware would then collect the victim's e-banking login credentials when he accessed his Internet banking account.

Control loopholes and lessons learnt

i. Bank customers are advised to stay alert to these scams by taking the following precautionary measures:

- Never click the hyperlinks or open the attachments in suspicious emails purporting to be sent by banks;
- Type the bank's website address, use a bookmarked link or use the bank's official mobile banking application to access its online services; and
- If in doubt, contact the bank's customer hotline or service centre to verify whether an email is actually sent by the bank.

ii. Banks should take the following measures to protect their customers from falling victim to these scams:

- Provide regular and effective cybersecurity alerts to their customers;

- Contact customers proactively if banks find that their customers have become a target of phishing scams;

- Report promptly the scam to the Hong Kong Monetary Authority and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force; and

- Report promptly the fraudulent websites to the Hong Kong Computer Emergency Response Team Coordination Centre and other channels as appropriate in order to block the public's access to these websites in a timely manner. Consider sharing relevant intelligence information with other banks through the Cyber Intelligence Sharing Platform.

Account takeover using a lost HKID card

This case involved a fraudster, having obtained the victim's lost HKID card, impersonating the victim and transferring a large sum of money from his account to a third-party account. The transfer was successful in part due to the deficiencies in the bank's customer identity verification process and also in part due to the victim failing to pay attention to an SMS notification sent by the bank.

Modus operandi / factors leading to the incident

The fraudster was in possession of the victim's lost HKID card. He went to the bank and impersonated the victim by showing the lost HKID card to enquire about the victim's bank account information (e.g. deposit types and balance). The fraudster then requested to make cash withdrawal of a small amount from the account. The teller checked the lost HKID card and verified the signature of the fraudster. She was unable to notice that the fraudster was not the account holder. She considered that the fraudster's appearance matched the photo shown on the

HKID card and his signature was the same as the specimen maintained in the bank's record.

After withdrawing a small amount of cash, the fraudster further requested to change the victim's contact telephone number in the bank's record. As a control measure against potential frauds, the bank sent an SMS notification to the victim's original contact telephone number to notify him of the change. Unfortunately, the victim overlooked the SMS message and took no action about it.

The next day, the fraudster went to another branch of the bank impersonating the victim again and requested for the early uplift of his time deposits and the transfer of the fund to a third-party account. As the amount involved was large, the branch manager conducted a call-back verification in addition to verifying the HKID card and signature provided by the fraudster. Since the contact telephone number in the bank's record had been changed, it was the fraudster, instead of the victim, answering the call-back. During the call, the branch manager confirmed the instructions with the fraudster without asking other questions to verify his identity. As a result, the fund was successfully transferred to the third-party account.

The account takeover by the fraudster was not discovered until the victim visited the bank two months later to renew his time deposits.

Control loopholes and lessons learnt

i. In this case, the branch manager and the teller had verified the identity and the signature of the fraudster. The former had also attempted to call back the victim. What he had not done, however, was to follow the bank's procedures and ask a few questions relating to the victim's personal particulars and account and transaction details (i.e. static and dynamic questions) during the call-back, given the amount of the transfer was large. If he had done so, the chance of the fraudster successfully transferring the fund to the third-party account would have been lowered.

ii. As for the victim, he should have notified the bank of the loss of his HKID card promptly so that the bank could take steps to protect his interest. Also, the victim should have paid attention to the SMS notification sent by the bank and contacted the bank as soon as practicable when the fraudster altered his personal record at the bank.